WE CLAIM:

1. A scalar multiplication calculation method for calculating a scalar multiplied point on the basis of a scalar value and a point on an elliptic curve in an elliptic curve cryptosystem, comprising the steps of:

judging a value of a bit of said scalar value; and

executing operations on said elliptic curve a predetermined number of times and in a predetermined order without depending on said judged value of said bit.

2. A scalar multiplication calculation method for calculating a scalar multiplied point on the basis of a scalar value and a point on an elliptic curve in an elliptic curve cryptosystem, comprising the steps of:

judging a value of a bit of said scalar value; and

executing addition on said elliptic curve and doubling on said elliptic curve in the order that said doubling on said elliptic curve is executed after said addition on said elliptic curve is executed.

3. A scalar multiplication calculation method for calculating a scalar multiplied point on the basis of a scalar value and a point on an elliptic curve in an elliptic curve cryptosystem, comprising the steps of:

judging a value of a bit of said scalar value; and

executing addition on said elliptic curve and doubling on said elliptic curve in the order that said addition on said elliptic curve is executed after said doubling on said elliptic curve is executed.

4. A scalar multiplication calculation method for calculating a scalar multiplied point on the basis of a scalar value and a point on an elliptic curve in an elliptic curve cryptosystem, comprising the steps of:

judging a value of a bit of said scalar value; and

executing addition on said elliptic curve and doubling on said elliptic curve simultaneously.

5. A scalar multiplication calculation method for calculating a scalar multiplied point on the basis of a scalar value and a point on an elliptic curve in an elliptic curve cryptosystem, comprising the steps of:

executing addition on said elliptic curve;

judging a value of a bit of said scalar value; and

executing doubling on said elliptic curve.

6. A scalar multiplication calculation method for calculating a scalar multiplied point on the basis of a scalar value and a point on an elliptic curve in an elliptic curve cryptosystem, comprising the steps

of:

randomizing calculation order of addition on said elliptic curve and doubling on said elliptic curve;

judging a value of a bit of said scalar value; and

executing said addition on said elliptic curve and said doubling on said elliptic curve in said order randomized by said step of randomizing calculation order of addition on said elliptic curve and doubling on said elliptic curve.

7. A scalar multiplication calculation method for calculating a scalar multiplied point on the basis of a scalar value and a point on an elliptic curve in an elliptic curve cryptosystem, comprising the steps of:

judging a value of a bit of said scalar value;

randomizing calculation order of addition on said elliptic curve and doubling on said elliptic curve; and

executing said addition on said elliptic curve and said doubling on said elliptic curve in said order randomized by said step of randomizing calculation order of addition on said elliptic curve and doubling on said elliptic curve.

8. A data generation method for generating second data from first data, comprising the step of

calculating a scalar multiplication by use of a scalar multiplication calculation method according to any one of Claims 1 to 7.

9. A signature generation method for generating signature data from data, comprising the step of calculating a scalar multiplication by use of a scalar multiplication calculation method according to any one of Claims 1 to 7.

10. A decryption method for generating decrypted data from encrypted data, comprising the step of calculating a scalar multiplication by use of a scalar multiplication calculation method according to any one of Claims 1 to 7.

11. A scalar multiplication calculator for calculating a scalar multiplied point on the basis of a scalar value and a point on an elliptic curve in an elliptic curve cryptosystem, comprising:

bit value judgement means for judging a value of a bit of said scalar value;

addition operation means for executing addition on said elliptic curve; and

doubling operation means for executing doubling on said elliptic curve;

wherein after the value of said bit of scalar value is judged by said bit value judgement means, said addition on said elliptic curve and said doubling on said elliptic curve are executed by said addition operation means and said doubling operation means a

predetermined number of times and in a predetermined order so as to calculate a scalar multiplied point.

12. A recording medium for storing a program relating to a scalar multiplication calculation method according to any one of Claims 1 to 7.

13. A scalar multiplication calculation method according to any one of Claims 1 to 7, wherein a Montgomery-form elliptic curve is used as said elliptic curve.

14. A scalar multiplication calculation method according to any one of Claims 1 to 7, wherein an elliptic curve defined on a finite field of characteristic 2 is used as said elliptic curve.